Release Notes for Cisco Secure Malware Analytics Appliance (formerly Threat Grid Appliance) Version 2.18

First Published: 2022-09-08

Last Modified: 2023-02-27

Introduction

This document describes the Release Notes, and Known Issues in Cisco Secure Malware Analytics (formerly Threat Grid) Appliance Version 2.18.0

User Documentation

The following Secure Malware Analytics (formerly Threat Grid) appliance user documentation is available:

Secure Malware Analytics Appliance User Documentation

Appliance user documentation is available on the Secure Malware Analytics appliance Install and Upgrade Guides page on the Cisco website.

Note Newer documentation is being made available from the Secure Malware Analytics appliance Products and Support page.

Backup FAQ

Please see the Backup Notes and FAQ for technical information and instructions.

Clustering Overview and FAQ

Please see the Clustering Overview and FAQ for additional information.

Installing Updates

Before you can update the Secure Malware Analytics (formerly Threat Grid) appliance with newer versions, you must have completed the initial setup and configuration steps as described in the Appliance Setup and Configuration Guide, which are available on the Secure Malware Analytics Appliance Install and Upgrade Guides page on the Cisco website.

New Appliances: If you have a new Appliance that shipped with an older version and wish to install updates, you must complete the initial configuration first. **Do Not** apply the updates until all Appliance configuration is done.

Appliance updates will not download unless the license is installed, and may not apply correctly if the Appliance has not been fully configured, including the database.

Secure Malware Analytics Appliance updates are applied through the Admin UI Portal.

Updates are one-directional: you cannot revert to a previous version after you upgrade to a more recent version.

To test the update, submit a sample for analysis.

Fixes and Updates

Version 2.18.1

This release increases the maximum size of sample to 250MB, addresses a scenario in which an internal data store enters a failed state when clustering is activated directly after NFS, adds masking of passwords found in logs, fixes syslog events transfer over the admin interface, rectifies log entry for LDAP logins and fix display of release notes.

- Increased the maximum sample size for submission from 100MB to 250MB.
- Fixed an issue where internal data store enters a failed state upon clustering activation directly after NFS.
- Masked sensitive information appearing in clear text in the logs.
- Fixed syslog over admin interface. Prior to this fix the syslog events where not sent out when syslog over admin interface was selected in opadmin.
- Fixed displaying the Release Notes in the opadmin update page.

Version 2.18.0

This release updates the core application software, adds support for Content Updates and new fast phishing and Win10 LTSC VMs, and includes a variety of other fixes and enhancements.

- The core application software and Behavioral Indicators (BIs) are updated to match cloud version 3.5.103. This includes the ability to download a sample report as PDF.
- Adds support for the new Content Update feature. Content updates are made available on a regular cadence and include essential behavioral indicators to increase efficacy.
- The Windows 10 (Phishing) VM facilitates URL phishing analysis that allows faster interactions compared to the Windows 10 browser VM. It prioritizes user experience over dynamic process monitoring.
- The Windows 10 LTSC (Long-Term Servicing Channel) VM functionality and features do not change over time.
- Fixed an issue with TLS certificate validation that validated a client CA certificate incorrectly using the server CA logic. It prevented client CAs from being added to the trust store unless they are considered server CAs.

Known Issues

- Firmware updates may sometimes fail to apply during the update process itself. Should this happen, these updates will be retried during the reboot process following any successful reconfiguration run.